

Patent Application of Y. Tsukamura for  
"Simplified Method of RSA" continued

12

CLAIMS

1. A method of digital signing on a digital message, comprising:
  - (a) providing a communication channel,
  - (b) providing a system authority means **O** which governs a private key **Do** and a public key **Eo**,  
where  
**Do**: private key of said system authority means **O** consisting of **do** and **no**  
in accordance with the RSA cryptographic method described in U.S.  
patent 4,405,829  
**do**: private exponent of said **Do**  
**Eo**: public key of said system authority means **O** consisting of **eo** and **no** in  
accordance with the RSA cryptographic method  
**eo**: public exponent of said **Eo**  
**no**: modulus of the key pair **Do**, **Eo**,
  - (c) providing at least one message sender means **Z** with an assigned ID # **Nz**,
  - (d) providing at least one message receiver means **Y**,
  - (e) said system authority means **O** providing **Cz** and said **Eo** to said **Z** and said **Eo**  
to said **Y**,  
where  
**Cz**: a secret key of said **Z** such that
$$\begin{aligned} \mathbf{Cz} &= \mathbf{Do} \{ \mathbf{Nz} \} \\ &= \mathbf{Nz}^{\mathbf{do}} \pmod{\mathbf{no}}, \end{aligned}$$
**{ }**: a cryptographic operation in accordance with the RSA cryptographic  
method,
  - (f) said **Z** providing a digital message **Mz** and transforming said **Mz** into a signed  
message **Sz** and then sending said **Nz**, said **Mz** and said **Sz** to said **Y** via said  
communication channel,  
where

Patent Application of Y. Tsukamura for  
“Simplified Method of RSA” continued

13

$$\begin{aligned} \mathbf{Sz} &= \mathbf{Mz} \{ \mathbf{Cz} \} \\ &= \mathbf{Cz}^{\mathbf{Mz}} \pmod{\mathbf{no}}, \end{aligned}$$

- (g) said **Y** receiving said **Nz**, said **Mz** and said **Sz**, and verifying said **Sz** by examining

$$\mathbf{Eo} \{ \mathbf{Sz} \} \text{ and } \mathbf{Nz}^{\mathbf{Mz}} \pmod{\mathbf{no}},$$

where

$$\mathbf{Eo} \{ \mathbf{Sz} \} = \mathbf{Sz}^{\mathbf{eo}} \pmod{\mathbf{no}},$$

whereby said message sender means **Z** can sign on said message **Mz** using less calculation than is necessary with the standard RSA cryptographic method, and said message receiver means **Y** can verify the genuineness of said signed message **Sz** without knowing said **Z**'s secret key **Cz**.

2. A method according to Claim 1 wherein said message sender means **Z**'s assigned ID # **Nz** includes information about its own expiration date, whereby said message receiver means **Y** can validate said assigned ID # **Nz**.
3. A method according to Claim 1 wherein said message sender means **Z** prepares pre-calculated tables of powers of said secret key **Cz**.
4. A method according to Claim 1 wherein said digital message **Mz** includes a hash value of information about an account balance.
5. A method according to Claim 1 wherein said digital message **Mz** includes information about the date of its own generation, whereby said digital message **Mz** is more difficult to duplicate.
6. A method of digital authentication, comprising:
  - (a) providing a communication channel,
  - (b) providing a system authority means **O** which governs a private key **Do** and a public key **Eo**,where

Patent Application of Y. Tsukamura for  
“Simplified Method of RSA” continued

14

**Do:** private key of said system authority means **O** consisting of **do** and **no** in accordance with the RSA cryptographic method described in U.S. patent 4,405,829

**do:** private exponent of said **Do**

**Eo:** public key of said system authority means **O** consisting of **eo** and **no** in accordance with the RSA cryptographic method

**eo:** public exponent of said **Eo**

**no:** modulus of the key pair **Do**, **Eo**,

- (c) providing at least one authenticator means **Y**,
- (d) providing at least one authenticatee means **Z** with an assigned ID # **Nz**,
- (e) said system authority means **O** providing **Cz** and said **Eo** to said **Z** and said **Eo** to said **Y**,

where

**Cz:** a secret key of said **Z** such that

$$\begin{aligned} \mathbf{Cz} &= \mathbf{Do} \{ \mathbf{Nz} \} \\ &= \mathbf{Nz}^{\mathbf{do}} \pmod{\mathbf{no}}, \end{aligned}$$

**{ }:** a cryptographic operation in accordance with the RSA cryptographic method,

- (f) said **Z** sending said **Nz** to said **Y** and requesting to be authenticated,
- (g) said **Y** generating a challenge message **Mz** and sending it to said **Z**,
- (h) said **Z** receiving said **Mz**, transforming it into a signed message **Sz** and sending said **Sz** to said authenticator means **Y** via said communication channel,

where

$$\begin{aligned} \mathbf{Sz} &= \mathbf{Mz} \{ \mathbf{Cz} \} \\ &= \mathbf{Cz}^{\mathbf{Mz}} \pmod{\mathbf{no}}. \end{aligned}$$

- (i) said **Y** receiving and verifying said **Sz** by examining **Eo** {**Sz**} and  $\mathbf{Nz}^{\mathbf{Mz}} \pmod{\mathbf{no}}$ ,

where

Patent Application of Y. Tsukamura for  
“Simplified Method of RSA” continued

15

$$\mathbf{E_o \{Sz\} = Sz^{e_o} \pmod{no},}$$

whereby said authenticatee means **Z** can be authenticated using less calculation than is necessary with the standard RSA cryptographic method, and said authenticator means **Y** can verify the genuineness of said signed message **Sz** without knowing said **Z**’s secret key **Cz**.

7. A method according to Claim 6 wherein said message sender means **Z**’s assigned ID # **Nz** includes information about its own expiration date, whereby said message receiver means **Y** can validate said **Nz**.
8. A method according to Claim 6 wherein said message sender means **Z** prepares pre-calculated tables of powers of said secret key **Cz**.
9. A method according to Claim 6 wherein said challenge message **Mz** includes information about the date of its own generation, whereby said **Mz** is more difficult to duplicate.
10. An authentication device that is used in a digital communication system, where said digital communication system comprises:
  - (a) a communications channel,
  - (b) a system authority means **O** for providing **Cx** and **Eo** to any entity **X** in the system,where
$$\begin{aligned}\mathbf{Cx:} & \text{ a secret key of said } \mathbf{X} \text{ such that} \\ & \mathbf{Cx = Do \{Nx\}} \\ & \mathbf{= Nx^{do} \pmod{no}}\end{aligned}$$
$$\{ \}: \text{ a cryptographic operation in accordance with the RSA cryptographic method described U.S. Patent 4,405,829}$$
$$\mathbf{Nx:} \text{ ID \# assigned to said } \mathbf{X}$$
$$\mathbf{Do:} \text{ private key of said system authority means } \mathbf{O} \text{ consisting of } \mathbf{do} \text{ and } \mathbf{no} \text{ in accordance with the RSA cryptographic method}$$
$$\mathbf{do:} \text{ private exponent of said } \mathbf{Do}$$

Patent Application of Y. Tsukamura for  
“Simplified Method of RSA” continued

16

**Eo:** public key of said system authority means **O** consisting of **eo** and **no** in accordance with the RSA cryptographic method

**eo:** public exponent of said **Eo**

**no:** modulus of the key pair **Do**, **Eo**,

(c) at least one message sender means **Z** coupled to said communication channel,

(d) at least one message receiver means **Y** coupled to said communication channel,

and said authentication devices is adapted for receiving said **Cx** and said **Eo** from said system authority means **O** and for transforming a digital message **M** to a signed message **S** and for transmitting said **S** via said communication channel,

where

$$S = M \{Cx\}$$

$$= Cx^M \pmod{no}.$$

11. A device according to Claim 10 wherein a table of the powers of said **Z**'s secret key **Cz** is prepared.